

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW MEXICO

FILED  
UNITED STATES DISTRICT COURT  
DISTRICT OF NEW MEXICO

03 APR 23 PM 3:49

JAMES SEABA and  
CORY PHILLIPS,

Plaintiffs,

v.

Civ. No. 02-103 LH/RHS

*Robert M. Marsh*  
CLERK-ALBUQUERQUE

MESOSYSTEMS TECHNOLOGY, INC.,

Defendant.

**AFFIDAVIT OF ANTON M. LITCHFIELD**  
**IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS**

STATE OF OREGON                     )  
  ) ss.  
COUNTY OF MULTNOMAH         )

Anton M. Litchfield, being first duly sworn upon oath, states as follows:

1. I am employed by New Technologies Armor, Inc. ("NTI"), a company specializing in the examination of computer-generated files and media. Since 1996, I have been conducting computer medium examinations with NTI and the Ontario Provincial Police of Toronto, Canada.

2. I have personal knowledge of the matters stated herein.

3. I submit this affidavit in support of Defendant's Motion to Dismiss Plaintiffs' Complaint and for Attorneys' Fees and Costs as a Sanction for Plaintiffs' Abuse of the Discovery Process.

4. NTI has been retained by MesoSystems Technology, Inc. ("MesoSystems") to maintain custody and control of two computer laptops and to conduct a factual examination of the activity on the hard drives of the laptops after December 6, 2001.

23

5. On February 12, 2002, NTI received two computer laptops belonging to MesoSystems. Both laptops were Sony Vaios. The first laptop was identifiable by serial number 28318330 3631178, which was used by James Scaba. The second laptop was identifiable by serial number 28318330 3631678, which was used by Cory Phillips.

6. When NTI received the two laptops from MesoSystems, the laptops were accompanied by a document entitled, "Chain of Custody Log." On February 12, 2002, a representative for NTI, Paul T. French, received the laptop computers from UPS and then placed the laptops in evidence storage. Mr. French subsequently initialed the chain of custody log. A true and correct copy of the Chain of Custody Log is attached hereto as Exhibit A. After the laptops were secured and stored in evidence storage, they were not accessed again until the examination of the hard drives began in January 2003.

7. In January 2003, NTI began its examination of the contents of the hard drives contained on the laptops. First, NTI made backup copies of the hard drives of each laptop. A backup copy is essentially an electronic fingerprint of the original hard drives and includes not only active files (normal files accessible to computer programs by their file name) but also areas of the hard drive where a trained specialist can find information of deleted data. After the backup copies were created, NTI returned the original hard drives to the laptops and returned the laptops to the secured storage room.

8. NTI conducted an examination of the backup hard drives from each laptop to determine their contents and the activity performed on them during the period between December 6, 2001, and January 30, 2002. In particular, NTI examined the data that was accessed between these dates and looked for evidence of files that may have been stored or accessed on removable media (e.g., floppy disk, CD, etc.).

9. The examination showed that both laptops had Microsoft Windows Millennium installed as the operating system. Windows Millennium tracks certain dates and times for files stored on its hard drive. Specifically, it tracks the date and time a file

is created on the hard drive (the time the file is saved on the hard drive), the modification date and time (the last time there was a change to the file), and the last access date.

10. The last access dates can be updated in several ways; however, they typically refer to the last time a user looked at the file or ran the program. With Microsoft Windows Millennium, if the file is deleted, the deleted file's last access date typically refers to the date the file was deleted. For example, if a user single-clicks the file "test.doc" with their mouse on 3/16/03, Windows then highlights the file. If the user then presses the shift+delete key, the file is then deleted. Using this process, the file is immediately deleted and does not go into the Recycle Bin. Using computer medium analysis, a trained individual can still look at the dates and times for the deleted file "test.doc." Even though the user in the example above never actually opened the file "test.doc" to view its contents, the simple fact of deleting it would update the last access date. Thus, when the file information for "test.doc" is reviewed, it would show that the file was deleted and that the last access date was 3/16/03.

11. Each hard drive in this case had two partitions that contained files. A partition is a logical division on a hard drive. If you had a single hard drive in your computer and it was partitioned in half, the user would see a C and a D drive. The examination of the contents of the hard drives revealed that on the first partition of Mr. Seaba's hard drive there were 37,495 files and folders that were still identifiable by the forensic software. To clarify this point: when a file is deleted in Windows Millennium, one of the things that occurs is that the directory entry (the file name/folder name) for the file/folder gets changed to flag the file/folder as deleted. This entry remains until it is overwritten by a new file/folder that is stored in the same directory position as the deleted entry. The index of the contents of the hard drives (files and folders) was made using forensics software that will identify active and deleted files that still have a directory entry. There were 116 identifiable files and folders found on the second partition of Mr. Seaba's hard drive. On Mr. Phillips' hard drive, there were

39,388 files and folders found on the first partition and 2,336 found on the second partition.

12. The index of the contents of the hard drives list the following columns of data:

- PATH (the directory structure in which the file\folder was found)
- FILE NAME (the name of the file)
- FILE-TYPE (if the file has an extension (e.g., .xls, .doc, etc.), it is listed in this column)
- DIR (indicates that the contents are a directory folder rather than a file)
- ARC (indicates that the file had an archive attribute)
- SYS (indicates that the file had a system attribute)
- HDN (indicates that the file had a hidden attribute)
- RO (indicates that the file had a read-only attribute)
- DEL (a "del" in this column indicates that the file has been deleted)
- SIZE (indicates the size of the file in bytes)
- LAST MODIFIED (the date the file was last modified)
- TIME (the time the file was last modified)
- CR-DATE (the date the file was created)
- CR-TIME (the time the file was created)
- LAST ACCESSED (the date the file was last accessed)
- FAT-Cluster (an alternative addressing method that can be used in the forensics examination)

13. After obtaining the full file lists for both laptops, I used Excel and Microsoft Access's capabilities of sorting and filtering to search for information related to files that were accessed, copied and/or deleted on or after December 6, 2001.

14. The kinds of file types contained on the hard drives, among others, are .doc files, .xls files, and .lnk files. .doc files are Microsoft Word files. .xls files are

Microsoft Excel files. .lnk files are shortcuts to the original files. When a user opens a particular file (e.g., a Microsoft Word document), Windows creates a shortcut to the original file, and the shortcut is stored as a .lnk file. The presence of a .lnk file is important because if a .lnk file has been created during the relevant time period in this case (December 6, 2001 through January 30, 2002), then it indicates that the users were opening or accessing files during that time.

15. Files on the hard drives that are stored in the "Temporary Internet Files" directory typically indicate that the files were saved automatically on the hard drive when the computer user was viewing them through Internet Explorer, which is a web-browser. There are two typical scenarios where this would occur. First, if a user browses a website that has a Word document linked on the site, the user could click on the document and view its contents. Second, if a user utilizes web-based email, such as Yahoo or Hotmail, and the user receives a Word document as an attachment, if the user opens the document, a copy of the document would be saved in the "Temporary Internet Files" directory.

16. NTI also looked for evidence of files being accessed from or copied to removable media (e.g., floppy disks and CDs). To do so, NTI identified .lnk files, which as described above, are shortcuts to the original file. If the shortcuts showed the path to the file as A:\, this indicates that the files were accessed from a floppy disk.

17. Both laptops contained evidence that Microsoft Office files were accessed from floppy disks. Like the index of the files and folders contained on the hard drives, NTI prepared a spreadsheet containing all of the files that were accessed from removable media, based on .lnk files. This only shows files that were accessed from a floppy disk. If a user were to copy files from their hard drive to a floppy disk and then never opened the file on the floppy disk, a .lnk file would not be created. This spreadsheet only reflected files that were actually opened from a floppy disk.

18. The examination of both hard drives indicated that numerous files were accessed and/or deleted after December 6, 2001.

19. The following is a summary of the files that were accessed and/or deleted from Seaba's computer after December 6, 2001, based on the results of the forensics software used that indexes the contents of hard drives:

- 829 files or folders were flagged as deleted from the first partition of the hard drive on or after December 6, 2001.
- 42 .doc files (Word documents) were accessed (i.e., opened) from the first partition of the hard drive on or after December 6, 2001, 4 of which were deleted on or after December 6, 2001.
- 44 .xls files (Excel spreadsheets) were accessed from the first partition of the hard drive on or after December 6, 2001, one of which was deleted on or after December 6, 2001.
- 595 .lnk files (shortcuts to files) were accessed from the first partition of the hard drive on or after December 6, 2001.
- 114 files or folders were accessed from the second partition of the hard drive on or after December 6, 2001, the majority of which were Microsoft Office files. 111 files or folders on the second partition were flagged as deleted on or after December 6, 2001.
- Based on the review of the .lnk files, two Microsoft Office files (.doc) were accessed from floppy disks on or after December 6, 2001.

20. The following is a summary of the files that were accessed and/or deleted from Phillips' computer between December 6, 2001 and January 30, 2002, based on the results of the forensics software used that indexes the contents of hard drives:

- 327 files or folders were flagged as deleted from the first partition of the hard drive on or after December 6, 2001.
- 94 .doc files were accessed from the first partition of the hard drive on or after December 6, 2001, with 49 flagged as deleted on or after December 6, 2001.
- 44 .xls files were accessed from the first partition of the hard drive on or after December 6, 2001, with 17 flagged as deleted on or after December 6, 2001.
- At least 440 .lnk files were accessed from the first partition of the hard drive on or after December 6, 2001, at least 18 of which were deleted on or after December 6, 2001.
- Based on a review of the .lnk files, 18 Microsoft Office documents were accessed from floppy disks and a CD-Rom called "Back-Up #1" on or after December 6, 2001. The drive letter associated with the CD-Rom was E:\, the same letter identified for the CD-Rom burner (see below).

21. There is no evidence that the computer used by Mr. Seaba was accessed after January 28, 2002. There is no evidence that the hard drive used by Mr. Phillips was accessed after January 24, 2002.

22. NTI also examined the hard drives to determine if Plaintiffs had used a CD-burner during the relevant time period. A CD-burner is a hardware device that allows users to burn (i.e., copy) files/folders to a CD-Rom. I reviewed the Windows registry on Mr. Phillips' laptop. The registry is comprised of two files that contain the computer's hardware and software configuration. Based on registry information found in \hkey\_local\_machine\Enum\Scsi, there was an entry for an HP CD-Writer+ 8200F. The registry also showed that the CD-burner's last drive letter assigned was E:\. I then viewed the information stored in Mr. Phillips' computer under C:\Program Files. This is the location where software is added to one's computer. Within that directory, I found a folder called \HP CD-Writer. Within this directory were files that allow a user to burn files to a CD. This folder was created on Mr. Phillips' computer on November 5, 2001. One of the directories within \HP CD-Writer was DirectCD, which is the same software that I use to burn CDs. The executable file (the file that launches the software) for DirectCD is DIRECTCD.EXE. The last access date for DIRECTCD.EXE on Mr. Phillips' computer was December 11, 2001.

23. I also checked Mr. Seaba's computer for the same information. Mr. Seaba's registry also had an entry showing an HP CD-Writer+ 8200f had been installed on it. The registry also showed that the last drive letter assigned to the CD-burner was E:\. Mr. Seaba's computer also had a folder called \HP CD-Writer in his C:\Program Files folder that was created on November 11, 2001. Mr. Seaba also had DirectCD on his computer and the last access date for the executable for DirectCD (DIRECTCD.EXE) was January 28, 2002.

24. I also examined the area of the hard drive that contains information related to items printed, namely C:\Windows\Spool\Printers. When you print an item in

Windows, the print job is spooled to the C:\Windows\Spool\Printers directory as a temporary file with a .spl extension. Spooling refers to the process of reading information in and storing it on the hard disk. This process is done to allow the computer to move onto other tasks. As it relates to printing, the computer spools the print job until the printer is ready to print. At the same time the .spl file is created, a .shd file is also created. The .shd file is called a shadow file and contains all the information required for the printer to re-submit the print job if the print job fails. The shadow file tracks, among other things, user name, document name, data type and what printer the job was sent to. By default, the spool and shadow files are deleted once the job prints. Based on information located in the deleted .shd files, I determined that the following files\items on Mr. Seaba's computer were printed on January 24, 2002:

- RTI\_MesoSystems\_1101.pdf
- Schedule\_1101.doc
- Agenda 11-19.doc
- Paper 352a.doc
- MesoFuelSuccessPlan.xls
- Travel Schedule.doc CJC 11-25-01
- HydrogenBulletin.doc
- BA010870053B Seaba v1
- And 50 Microsoft Outlook Items

25. I then reviewed Mr. Phillips printer information. Many of the .shd files had been overwritten so I could not determine what had been printed. Based on deleted .shd files that I could examine, I determined that on November 28, 2001, the following item was printed from Mr. Phillips' computer:

- Air Force Solicitations.doc

On November 11, 2001 the following item was printed from Mr. Phillips' computer:



- <http://www.svce.ac.in/~msubbu/LectureNotes/PetroleumTech/SulfurOxygenNitrogen.htm>

On December 3, 2001, the following items were printed from Mr. Phillips' computer:


- <http://www.lanl.gov/projects/cetc/factsheets/noxso/remflugasdemo.html>
- <http://process-economics.com/Reports/peprpt063.htm>
- <http://www.iea-coal.org.uk/CCI/database/fgd.htm>

26. In addition to identifying the files stored on the hard drives, NTI recovered some files that had been deleted. Computer media examination specialists can recover deleted files provided that the file has not been overwritten by new data. Using specialized computer software, NTI recovered fifteen previously deleted Microsoft Office files from Seaba's laptop and nineteen previously deleted Microsoft Office files from Phillips' laptop. The following is a list of some of the files NTI recovered (some, but not all, of which were deleted):

- File name: L.D.-Memo.11.01.doc, last accessed on Seaba's hard drive on December 7, 2001. This file was deleted. A true and correct copy of the L.D.-Memo.11.01.doc is attached hereto as Exhibit B. The date shown on this document is not the true date the document was created. Instead, it shows the date the document was opened and printed after it was recovered from the hard drive. This is the result of a date field in the document that automatically updates the date when it is printed.
- File name: Levi 11-23 Memo #2.doc, last accessed on Seaba's hard drive on December 7, 2001 and Phillips' hard drive on November 30, 2001. Both of these files were deleted. A true and correct copy of the Levi 11-23 Memo #2.doc accessed on Seaba's and Phillips' computers are attached hereto as Exhibits C and D, respectively. For the reasons listed above, the date shown on this document is also not indicative of when it was created.

- File name: MesoSystems task report.doc, last accessed on Seaba's hard drive on December 7, 2001. This file was deleted. A true and correct copy of the MesoSystems task report.doc is attached hereto as Exhibit E.
- File name: MmdkRedPathproposal112801-draft4.doc, last accessed on Seaba's hard drive December 7, 2001. This file was deleted. A true and correct copy of the MmdkRedPathproposal112801-draft4.doc is attached hereto as Exhibit F.
- File name: Red Path BP.12.1.01.doc, last accessed on Seaba's hard drive on December 7, 2001. This file was deleted. For exhibit page limit constraint purposes, a true and correct copy of the first page of the file entitled Red Path BP.12.1.01.doc is attached hereto as Exhibit G.
- File name: MesoFuel Expense Projections Alpha Phase 6-02v1.xls, last accessed on Seaba's hard drive on December 22, 2001 and on Phillips' hard drive on December 7, 2001. These files were not deleted from either laptop. A true and correct copy of the MesoFuel Expense Projections Alpha Phase 6-02v1.xls is attached hereto as Exhibit H.
- File name: MesoFuel Expense Projections Alpha Phase 6-02.xls, last accessed on Phillips' hard drive on December 7, 2001. This file was not deleted. A true and correct copy of the MesoFuel Expense Projections Alpha Phase 6-02.xls is attached hereto as Exhibit I.
- File name: BA010870053B SEABAv1.doc, last accessed on Seaba's hard drive on December 7, 2001. This file was deleted. For exhibit page limit constraint purposes, a true and correct copy of the first page of the file entitled BA010870053B SEABAv1.doc is attached hereto as Exhibit J.
- File name: NDA Team Specialty.doc, last accessed on Phillips' hard drive on December 7, 2001. This file was deleted. A true and correct copy of the NDA Team Specialty.doc is attached hereto as Exhibit K.

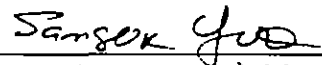
- File name: Summary of Events.doc, last accessed on Phillips' hard drive on December 7, 2001. This file was not deleted. A true and correct copy of the Summary of Events.doc is attached hereto as Exhibit I.

  
Anton M. Litchfield

**STATE OF OREGON  
COUNTY OF MULTNOMAH**

SUBSCRIBED and SWORN to before me this 22 day of April, 2003.



  
Print Name: SANG OK YOO  
Notary Public in and for the State of Oregon,  
residing at Gresham, OR  
My commission expires: 10/17/03

I HEREBY CERTIFY that a true  
and correct copy of the foregoing  
was ~~presented~~ <sup>hand delivered</sup> to counsel of record  
this 23<sup>rd</sup> day of April, 2003.

  
Alberto A. León

**THE EXHIBITS ATTACHED TO  
THIS PLEADING ARE TOO  
VOLUMINOUS TO SCAN. SAID  
EXHIBITS ARE ATTACHED TO THE  
ORIGINAL PLEADING IN THE CASE  
FILE WHICH IS LOCATED IN THE  
RECORDS DEPARTMENT, U.S.  
DISTRICT COURT CLERK'S  
OFFICE...**